УДК 343.985

А. В. Сычева
старший преподаватель кафедры криминалистики
учебно-научного комплекса по предварительному
следствию в органах внутренних дел
Волгоградской академии МВД России,
кандидат юридических наук

К ВОПРОСУ ОБ АКТУАЛЬНЫХ СПОСОБАХ СОВЕРШЕНИЯ «ДИСТАНЦИОННОГО» МОШЕННИЧЕСТВА

Согласно статистическим данным МВД России за январь–февраль 2021 года, в Российской Федерации снизилось общее количество зарегистрированных преступлений. Но при этом значительно возросло количество преступлений, совершенных дистанционно: в частности, количество IT-преступлений возросло на 29,4 % по сравнению с аналогичным периодом прошлого года; преступлений, совершенных с использованием сети Интернет, — на 48,3 %; преступлений, совершенных при помощи средств мобильной связи, — на 32,6 % [1]. Немалая часть данных преступных посягательств совершается путем обмана или злоупотребления доверием (так называемые дистанционные мошенничества). При этом преступники не просто изобретают новые способы обмана граждан, но и совершенствуют уже существующие.

Важно отметить, что значительная часть указанных преступлений не выявляется в силу конспиративных возможностей злоумышленников либо отсутствия сообщений о преступлениях со стороны потерпевших, а часть регистрируется как правонарушения по причине малозначительного ущерба, что также является проблемной стороной исследуемого вопроса [2].

Рассмотрим некоторые актуальные способы совершения «дистанционного» мошенничества.

1. Мошенничества с использованием сайтов-двойников. Как известно, мошенники уже давно используют сайты объявлений в Интернете о продаже или сдаче в аренду имущества («Авито», «Юла», «Циан» и др.). В связи с этим указанные сервисы предприняли меры для того, чтобы обезопасить своих клиентов. В частности, сервис «Авито» дает возможность общения продавца с покупателем только посредством звонков и сообщений на своем сайте или в приложении. В приложении установлен запрет на отправку сообщений, содержащих номера телефонов, банковских карт и т. д. Кроме этого, сервис «Авито» создал свою доставку, при которой продавец получает деньги от продажи только тогда, когда покупатель заберет товар из пункта выдачи и подтвердит заявленные характеристики товара. Сервис «Юла» также предпринял меры для обеспечения

безопасности своих клиентов, введя видеозвонки и прямую связь через свое приложение.

Несмотря на указанные меры, мошенники уже разработали новый способ обмана. Совершая покупку товара через сервис объявлений «Авито», продавец может предложить покупателю выслать платежный документ. Преступник отправляет покупателю ссылку на оплату товара. Покупатель, перейдя по указанной преступником ссылке, вводит данные своей карты для совершения платежа, и когда банк одобряет совершение платежной операции, продавец блокирует покупателя и пропадает. При переходе по полученной от мошенника ссылке жертва попадает на специально созданный фишинговый сайт, визуально похожий на «Авито». Подобные сайты мошенники создают не только у онлайн-платформ, но и у официальных ведомств России.

Так, 12 января 2021 г. А., желая совершить покупки на официальном сайте IHerb, установила соответствующее приложение посредством сервиса Google Play. О том, что весной 2020 года официальное приложение IHerb было удалено из российского App Store и Google Play, она не знала. Введя запрос IHerb в поисковой строке сервиса Google Play, она увидела несколько вариантов искомого приложения, которые визуально были похожи на оригинальное, но отличались друг от друга какими-либо деталями. Когда А. установила одно из предложенных приложений, ей было предложено войти в ее аккаунт, используя номер телефона и временный код подтверждения. После ввода указанного кода в приложении с банковской карты А. было списано 45 000 рублей.

При вводе кода подтверждения мошенники получают доступ к паспортным и платежным данным жертвы, а значит, получают возможность распоряжаться данной информацией по своему усмотрению. Кроме этого, фишинговые приложения получают доступ к IHerb-аккаунту жертвы и ее вознаграждениям, если таковые имеются, которыми они также смогут пользоваться в целях личной выгоды [3].

2. Движение денежных средств на банковских картах. Всем давно известен способ совершения мошенничества, когда преступник звонит по телефону жертве и, представляясь сотрудником банка, получает информацию о данных карты жертвы и в дальнейшем похищает денежные средства последней.

Так как мошенники понимают, что данный способ уже всем известен и зачастую перестал работать, они его немного видоизменили. Преступники звонят по телефону жертве и представляются сотрудниками службы безопасности банка. При этом якобы сотрудник сообщает жертве о подозрительном запросе на списание денежных средств со счета жертвы, которое последняя не совершала. В целях завоевания доверия жертвы преступник называет личные данные последней, количество банковских карт, которыми жертва владеет, и даже может

назвать точный адрес отделения банка, из которого якобы поступил звонок. При этом мошенник спокойным тоном отвечает на все вопросы жертвы. Далее преступник просит перевести всю сумму с карты жертвы на якобы страховой счет, принадлежащий банку-партнеру. Ранее при совершении мошенничеств таким способом преступники, как правило, не давали жертве времени раздумывать, сразу настоятельно рекомендовали сообщить ПИН-код карты, ее номер и т. д. В данном случае преступники ведут себя спокойно, никаких требований не предъявляют, чем еще больше располагают к себе. Жертва сама осуществляет перевод своих денежных средств на счет мошенника. Преступник при этом утверждает, что деньги вернутся на счет жертвы в течение получаса, но этого не происходит. Только по истечении указанного промежутка времени человек понимает, что стал жертвой обмана [4].

3. Проверка iPhone через Apple ID во время продажи. Существует мнение, что iPhone — один из самых безопасных смартфонов, так как у них нет вирусов, на них регулярно приходят обновления, а также существует защита личных данных пользователей. Но даже к таким, казалось бы, безопасным смартфонам мошенники нашли свой подход.

Так, С., используя сервис «Авито», разместила объявление о продаже своего старого смартфона iPhone. Ей сразу же позвонила девушка и сообщила, что желает его приобрести в этот же день, но у нее возникли технические проблемы с Apple ID [5]. Девушка попросила жертву войти в ее учетную запись через свой телефон и проверить, все ли в порядке. С., не подозревая об обмане, вошла в Apple ID мошенницы. Через несколько минут был заблокирован телефон и включена функция поиска, которая издает громкие и непрекращающиеся звуки. Мошенница потребовала от жертвы срочно перевести ей 10 000 руб., чтобы разблокировать телефон [6].

Перечисленные способы совершения «дистанционных» мошенничеств, безусловно, не являются исчерпывающими, существуют и многие другие. Мошенники не стоят на месте, придумывают все новые, более изощренные способы обмана.

Рассмотренные нами способы совершения «дистанционных» мошенничеств являются криминалистически значимой информацией, которая может быть полезной для органов предварительного расследования при раскрытии и расследовании преступлений, выдвижении и проверке следственных версий, выборе средств и методов расследования преступлений.

---

1. Краткая характеристика состояния преступности в Российской Федерации за январь–февраль 2021 года [Электронный ресурс] // Официальный сайт Министерства внутренних дел Российской Федерации. URL: https://мвд.рф/reports/item/23447482/ (дата обращения: 29.03.2021). Перейти к источнику Вернуться к статье

2. Богданов А. В., Ильинский И. И., Хазов Е. Н. Киберпреступность и дистанционное мошенничество как одна из угроз современному обществу // Криминологический журнал. 2020. № 1. С. 15–20. Вернуться к статье

3. Материалы следственной практики ГСУ ГУ МВД России по г. Москве. Вернуться к статье

4. Развод чистой воды: Как обманывают мошенники в 2020 году? [Электронный ресурс] // СМИ сетевое издание 5-tv.ru. URL: https://www.5-tv.ru/news/284761/razvod-cistoj-vody-kak-obmanyvaut-mosenniki-v2020-godu/ (дата обращения 28.03.2021). Перейти к источнику Вернуться к статье

5. Apple ID [Электронный ресурс] // Свободная энциклопедия Википедия. URL: https://ru.wikipedia.org/wiki/Apple_ID (дата обращения 29.03.2021). Перейти к источнику Вернуться к статье

6. Материалы следственной практики СУ МВД России по Тюменской области. Вернуться к статье